Fonctions arithmétiques

B.S.

21 juillet 2017

1 Généralités

Définition 1 (Fonction arithmétique)**.** *Soit A un anneau commutatif. On nomme fonction arithmétique (à valeurs dans A) une fonction $\mathbb{N}^* \to E$. L'ensemble des fonctions arithmétiques à valeurs dans A est noté $F(A)$.*

Définition 2 (Fonction (complètement) multiplicative)**.** *Soit une fonction arithmétique f à valeurs dans l'anneau commutatif A. On dit que la fonction est :*

- *multiplicative lorsque $f(1) = 1_A$ et que pour tous entiers p et q premiers entre eux, $f(pq) = f(p)f(q)$ (on dit alors $f \in F_m(A)$) ;*
- *complètement multiplicative lorsque $f(1) = 1_A$ et que pour tous entiers p et q, $f(pq) = f(p)f(q)$ (on dit alors $f \in F_{cm}(A)$)*

Propriété 1. *Une fonction complètement multiplicative est déterminée par sa restriction à $\mathcal{P}$ (l'ensemble des nombres premiers). Une fonction multiplicative est déterminée par sa restriction à $\{p^k \mid p \in \mathcal{P}, k \geq 1\}$.*

Définition 3 (Convolution de Dirichlet)**.** *Soit f et g deux fonctions arithmétiques à valeurs dans un même anneau commutatif A. On définit la fonction arithmétique $f \star g$ par la relation :*

$$(f \star g)(n) = \sum_{pq=n} f(p)g(q)$$

où la somme parcourt l'ensemble des couples de diviseurs positifs de n de produit n.
On peut aussi écrire

$$(f \star g)(n) = \sum_{k|n} f(k)g\left(\frac{n}{k}\right).$$

Cela définit une loi de composition interne sur l'ensemble des fonctions arithmétiques à valeurs dans A, qui est manifestement commutative et bilinéaire.

Propriété 2. *$\star$ admet 0 comme élément absorbant et $\chi_{\{1\}}$ (noté δ) comme élément neutre.*

Preuve 1.

$$(f \star 0)(n) = \sum_{pq=n} f(p) \times 0 = 0$$

$$(f \star \delta)(n) = \sum_{pq=n} f(p) \times \delta_{q1} = f(n)$$

Propriété 3. *Le produit de convolution de deux fonctions multiplicatives est multiplicatif.*

Preuve 2. *Soit f et g multiplicatives et p et q premiers entre eux.*

$$\begin{aligned}
(f \star g)(pq) &= \sum_{k|pq} f(k)g\left(\frac{pq}{k}\right) \\
&= \sum_{k|p,l|q} f(kl)g\left(\frac{pq}{kl}\right) \\
&= \sum_{k|p,l|q} f(k)f(l)g\left(\frac{p}{k}\right)g\left(\frac{q}{l}\right) \\
&= \left(\sum_{k|p} f(k)g\left(\frac{p}{k}\right)\right)\left(\sum_{l|q} f(l)g\left(\frac{q}{l}\right)\right) \\
&= (f \star g)(p) \times (f \star g)(q).
\end{aligned}$$

Propriété 4. *$\star$ est associative.*

Preuve 3.

$$\begin{aligned}((f\star g)\star h)(n) &= \sum_{pq=n}(f\star g)(p)h(q)\\ &= \sum_{pq=n}\sum_{rs=p} f(r)g(s)h(q)\\ &= \sum_{prs=n} f(r)g(s)h(q)\end{aligned}$$

Cette dernière expression est égale à $(f\star(g\star h))(n)$ par le même calcul, d'où le résultat.

Ainsi, $F(A)$ a une structure d'anneau commutatif pour les lois $+,\star$.

Propriété 5. *Si f est complètement multiplicative, alors pour toutes fonctions g et h :*

$$(fg)\star(fh) = f(g\star h)$$

Preuve 4.

$$(fg)\star(fh)(n) = \sum_{pq=n} f(p)g(p)f(q)h(q) = \sum_{pq=n} f(pq)g(p)h(q) = f(n)(g\star h)(n)$$

2 Chasse aux inverses

2.1 Cas général

Une fonction arithmétique f est inversible lorsqu'il existe une fonction arithmétique g telle que :

$$f\star g = \delta$$

C'est-à-dire que :

$$f(1)g(1) = 1$$

$$\forall n\geq 2, \sum_{k|n} f(k)g\left(\frac{n}{k}\right) = 0$$

La première condition nous donne immédiatement la condition nécessaire suivante : si f est inversible, alors $f(1)$ est inversible dans A.

Cette condition est en outre suffisante : en effet, il suffit alors de calculer récursivement :

—

$$g(1) = f(1)^{-1}$$

—

$$g(n) = -f(1)^{-1}\left(\sum_{k|n,k>1} f(k)g\left(\frac{n}{k}\right)\right)$$

D'où le théorème suivant :

Théorème 1. *Une fonction $f\in F(A)$ est inversible si et seulement si $f(1)\in A^\times$, et on peut alors calculer récursivement l'inverse.*

2.2 Cas multiplicatif

Dans le cas multiplicatif, $f(1) = 1$ donc les fonctions sont toujours inversibles. Reste à déterminer si leur inverse est toujours multiplicatif.

Soit donc $f\in F_m(A)$ et $g = f^{-1}$. Supposons par l'absurde qu'on ait p, q deux entiers premiers entre eux, strictement supérieurs à 1 (sans quoi le résultat est clair), et tels que pq soit un contrexemple minimal.

$$\begin{aligned}
g(pq) &= -\sum_{k|p,l|q,kl>1} f(k)f(l)g\left(\frac{p}{k}\right)g\left(\frac{q}{l}\right) \\
&= -\sum_{l|q,l>1} f(1)f(l)g(p)g\left(\frac{q}{l}\right) \\
&\quad -\sum_{k|p,k>1}\sum_{l|q} f(k)f(l)g\left(\frac{p}{k}\right)g\left(\frac{q}{l}\right) \\
&= -f(1)g(p)[(f\star g)(q) - f(1)g(q)] \\
&\quad -(f\star g)(q)[(f\star g)(p) - f(1)g(p)] \\
&= -g(p)[0-g(q)] - 0[0-g(p)] \\
&= g(p)g(q)
\end{aligned}$$

Par l'absurde, on a donc montré que l'inverse est toujours multiplicatif.

Théorème 2. *Si f est multiplicative, alors f est inversible et son inverse est multiplicatif. $F_m(A)$ a donc une structure de groupe pour $\star$.*

2.3 Exemples

2.3.1 Exemple fondamental

Soit 1 la fonction constante égale à 1. Clairement multiplicative, elle est inversible. Déterminons la valeur de son inverse, noté μ, en les $p^k, p \in \mathcal{P}, k \geq 1$.

$$\mu(1) = 1$$
$$\mu(p) = -\sum_{k|p,k<p} \mu(k) = -\mu(1) = -1$$
$$\mu(p^2) = -\sum_{k|p^2,k<p^2} \mu(k) = -\mu(1) - \mu(p) = -1 + 1 = 0$$

De même on montre, dès que $k \geq 2$:

$$\mu(p^k) = -\sum_{i=0}^{k-1} \mu(p^i) = -\sum_{i=0}^{k-2} \mu(p^i) - \mu(p^{k-1}) = \mu(p^{k-1}) - \mu(p^{k-1}) = 0$$

Ainsi, si on a un entier n quelconque décomposé en facteurs premiers, alors dès qu'une valuation est supérieure ou égale à 2 (c'est-à-dire que n est divisible par un carré différent de 1), son image par μ est nulle. Sinon, son image vaut $(-1)^r$ où r est le nombre de facteurs premiers distincts de n. On nomme μ la fonction de MOEBIUS.

2.3.2 Fonctions complètement multiplicatives

Soit f complètement multiplicative. On remarque que :

$$f\star(f\mu) = (f1)\star(f\mu) = f(1\star\mu) = f\delta = \delta$$

où on a utilisé $f(1) = 1$. Ainsi $f^{-1} = f\mu$.

2.3.3 Nombre de diviseurs

Soit $d : n \mapsto \sum_{k|n} 1$ la fonction nombre de diviseurs. On peut écrire $d = 1\star 1$ et donc $d^{-1} = \mu\star\mu$.

$$(\mu\star\mu)(p^k) = \sum_{i=0}^{k} \mu(p^i)\mu(p^{k-i}) = 1\mu(p^k) - 1\mu(p^{k-1})$$

Ainsi si $k \geq 3$, $(\mu\star\mu)(p^k)$ est clairement nul. Sinon, cela dépend :

$$(\mu\star\mu)(p^2) = \mu(p^2) - \mu(p) = 0 + 1 = 1$$

$$(\mu\star\mu)(p) = \mu(p) - 1 = -2$$

Soit donc un entier n. S'il est divisible par un cube distinct de 1, son image par d^{-1} est nulle. Sinon, on écrit $n = M^2\prod_{i\leq r} p_i$ et alors $d^{-1}(n) = (-2)^r$

2.3.4 Somme des diviseurs

Soit $\sigma : n \mapsto \sum_{k|n} k$ la fonction somme des diviseurs. On peut écrire $\sigma = Id \star 1$ donc σ est multiplicative, et $\sigma^{-1} = (Id\mu) \star \mu$.

Ainsi, pour $k \geq 1$:

$$\sigma^{-1}(p^k) = \sum_{i \leq k} p^i \mu(p^i)\mu(p^{k-i}) = \mu(p^k) - p\mu(p^{k-1})$$

D'où $\sigma^{-1}(p^0) = 1$, $\sigma^{-1}(p^1) = -p - 1$, $\sigma^{-1}(p^2) = 0 + p = p$, $\sigma^{-1}(p^k) = 0, k \geq 3$.

Soit n un entier. Si n est divisible par un cube distinct de 1, son image par σ^{-1} est nulle. Sinon, on écrit $n = N^2 \prod_{1 \leq i \leq r} p_i$ et alors

$$\sigma^{-1}(n) = (-1)^r N \prod_{1 \leq i \leq r} (p_i + 1)$$

3 Série de Dirichlet

On s'intéresse désormais au cas des fonctions arithmétiques à valeurs dans $\mathbb{C}$.

À une fonction f, on associe la fonction $Sf : U \to \mathbb{C}$ qui à tout s tel que la série converge associe $\sum_n \frac{f(n)}{n^s}$.

On remarque que :

$$\sum_n \frac{f(n)}{n^s} \sum_m \frac{g(m)}{m^s} = \sum_n \sum_m \frac{f(n)g(m)}{(nm)^s} = \sum_p \frac{1}{p^s} \left(\sum nm = pf(n)g(m) \right) = \sum_p \frac{(f \star g)(p)}{p^s}$$

On en déduit : $Sf \times Sg = S(f \star g)$. On retrouve ainsi des résultats comme $\frac{1}{\zeta(s)} = \sum \frac{\mu(n)}{n^s}$. De plus :

$$Sf(s-t) = \sum_n \frac{n^t f(n)}{n^s} = S(Id^t f)(s)$$

Ainsi, par exemple, calculer $\frac{\zeta(s-r)}{\zeta(s)}$ revient à calculer $S(Id^r \star \mu)$.

3.1 Cas multiplicatif

Soit f multiplicative. En décomposant chaque n comme un produit de facteurs premiers et en disjoignant pour chaque p selon sa valuation :

$$Sf(s) = \sum_n \frac{f(n)}{n^s} = \prod_{p \in \mathcal{P}} \left(1 + \sum_{k \geq 1} \frac{f(p^k)}{p^{sk}} \right)$$

3.2 Cas complètement multiplicatif

Soit f complètement multiplicative. En reprenant le calcul précédent (série géométrique) :

$$Sf(s) = \prod_{p \in \mathcal{P}} \left(\frac{p^s}{p^s - f(p)} \right)$$

4 Fonctions totient et indicatrice d'Euler

Soit $J_r = Id^r \star \mu$. C'est une fonction multiplicative.

$$J_r(p^k) = \sum_{0 \leq i \leq k} p^{r(k-i)} \mu(p^i) = p^{rk} - p^{r(k-1)} = p^{rk} \left(1 - \frac{1}{p^r} \right)$$

Donc, pour un $n = \prod p_i^{n_i}$ quelconque, $J_r(n) = n^r \prod_i \left(1 - \frac{1}{p_i^r} \right)$. On remarque en outre que $J_r \star 1 = Id^r \star \mu \star 1 = Id^r$, c'est-à-dire que :

$$\sum_{k|n} J_r(k) = n^r$$

On a $SJ_r(s) = \frac{\zeta(s-r)}{\zeta(s)}$ d'après le calcul ci-dessus.

Plaçons nous dans le cas d'un entier $k \geq 1$ et montrons que J_k est le nombre de k-uplets $a_1, \ldots, a_k$ de $\{1, \ldots, n\}$ tels que $a_1, \ldots, a_k, n$ soient premiers entre eux (dans leur ensemble).

Il y a n^k k-uplets de $\{1, \ldots, n\}$. Soit $a_1, \ldots a_k$ un tel k-uplet tiré uniformément au hasard. La probabilité que $a_1, \ldots, a_k, n$ soient premiers entre eux est la probabilité que pour tout diviseur premier p de n, p ne divise pas à la fois $a_1, \ldots, a_k$. Il est aisé de vérifier que les événements "p divise à la fois $a_1, \ldots, a_k$" ($p|n$, p premier) sont indépendants (par récurrence, en divisant $a_1, \ldots, a_k$ par le diviseur commun à chaque fois), et donc la probabilité cherchée vaut $\prod(1 - \frac{1}{p^k})$ d'où le résultat.

On sait donc que $J_1(n)$ est également $\varphi(n)$, où φ est la fonction indicatrice d'Euler, qui compte le nombre d'entiers inférieurs à n premiers avec n. On retrouve ainsi le résultat classique :

$$\sum_{k|n} \varphi(k) = n.$$

5 Caractères de Dirichlet et fonctions L